UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/627,158	07/25/2003	Adrian Patrick Kent	200206289-1	2520

22879 7590 04/16/2008

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
POPHAM, JEFFREY D	

ART UNIT	PAPER NUMBER
2137	

NOTIFICATION DATE	DELIVERY MODE
04/16/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
mkraft@hp.com
ipa.mail@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/627,158
Filing Date: July 25, 2003
Appellant(s): KENT ET AL.

Charles W. Griggers
Reg. #47,283
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 1/14/2008 appealing from the Office action mailed 7/13/2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

Bennett et al., "Experimental Quantum Cryptography", 9/1991, pp. 1-28

Sych et al., "Quantum cryptography with a continuous alphabet", 4/4/2003, pp. 1-14

Black et al., "Quantum Computing and Communication", 2/20/2002, pp. 1-52

6,678,450 FRANSON 1/2004

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-7, 10-13, 16-20, 22-24, 26-38, 41-43, and 46-49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bennett (Bennett et al., "Experimental Quantum Cryptography", 9/1991, pp. 1-28) in view of Sych (Sych et al., "Quantum cryptography with continuous alphabet", 4/4/2003, pp. 1-14).

Regarding Claim 1,

> Bennett discloses a method of establishing a shared secret random cryptographic key between a sender and a recipient using a quantum communications channel, the method comprising:

Generating a plurality of random quantum states of a quantum entity, each random state being defined by a randomly selected one of a first plurality of bases in Hilbert space (Section 2; note pages 4-5);

Transmitting the plurality of random quantum states of the quantum entity via the quantum channel to the recipient (Section 2; note pages 4-5);

Measuring the quantum state of each of the received quantum states of the quantum entity with respect to a randomly selected one of a second plurality of bases in Hilbert space (Section 2; note pages 4-5);

Transmitting to the recipient composition information describing a subset of the plurality of random quantum states (Section 2; note pages 4-5);

Analyzing the received composition information and the measured quantum states corresponding to the subset to derive a first statistical distribution describing the subset of transmitted quantum states and a second statistical distribution describing the corresponding measured quantum states (Section 2; note pages 4-5);

Establishing the level of confidence in the validity of the plurality of transmitted random quantum states by verifying that the first and second statistical distributions are sufficiently similar (Section 2; note pages 5-6);

Deriving a first binary string and a second binary string correlated to the first binary string, respectively from the transmitted and received

plurality of quantum states not in the subset (Section 2; note pages 5-6); and

Carrying out a reconciliation of the second binary string to the first binary string by using error correction techniques to establish the shared secret random cryptographic key from the first and second binary strings (Section 2; note pages 6-7);

But does not disclose the first plurality of bases being randomly and independently chosen from a uniform distribution of all pure quantum states in Hilbert space and the second plurality of bases being randomly and independently chosen from a uniform distribution of all pure quantum states in Hilbert space.

Sych, however, discloses the first plurality of bases being randomly and independently chosen from a uniform distribution of all pure quantum states in Hilbert space and the second plurality of bases being randomly and independently chosen from a uniform distribution of all pure quantum states in Hilbert space (Pages 4-8, section III). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the continuous quantum alphabet of Sych into the QKD system of Bennett in order to improve the critical QBER (Quantum Bit Error Rate), allow secure data transmission through practically any noisy quantum channel, and/or allow the system to work at basically any level of external errors or eavesdropping attacks.

Regarding Claim 26,

Claim 26 is a method claim that is broader than method claim 1 and is rejected for the same reasons.

Regarding Claim 35,

Claim 35 is a method claim that is broader than method claim 1 and is rejected for the same reasons.

Regarding Claim 2,

Bennett as modified by Sych discloses the method of claim 1, in addition, Bennett discloses that the first and second plurality of bases in Hilbert space each comprise at least four random bases (Section 2, note pages 4-5); and Sych discloses that the first and second plurality of bases in Hilbert space each comprise at least four random bases (Pages 4-8, section III).

Regarding Claim 27,

Claim 27 is a method claim that is broader than method claim 2 and is rejected for the same reasons.

Regarding Claim 36,

Claim 36 is a method claim that is broader than method claim 2 and is rejected for the same reasons.

Regarding Claim 3,

Bennett as modified by Sych discloses the method of claim 1, in addition, Bennett discloses that the selecting step comprises generating

and measuring a first plurality of bases in two-dimensional Hilbert space (Section 2, note pages 4-5; and Section 3, note page 10); and Sych discloses that the selecting step comprises generating and measuring a first plurality of bases in two-dimensional Hilbert space (Pages 4-8, section III).

Regarding Claim 28,

Claim 28 is a method claim that is broader than method claim 3 and is rejected for the same reasons.

Regarding Claim 4,

Bennett as modified by Sych discloses the method of claim 1, in addition, Bennett discloses that the selecting step comprises generating and measuring a first plurality of bases in a real subspace of two-dimensional Hilbert space (Section 2, note pages 4-5).

Regarding Claim 29,

Claim 29 is a method claim that is broader than method claim 4 and is rejected for the same reasons.

Regarding Claim 5,

Bennett as modified by Sych discloses the method of claim 1, in addition, Bennett discloses that the composition information transmitting step comprises transmitting information describing the bases of the subset of the plurality of random quantum states (Section 2, note pages 4-5).

Regarding Claim 30,

Claim 30 is a method claim that is broader than method claim 5 and is rejected for the same reasons.

Regarding Claim 6,

Bennett as modified by Sych discloses the method of claim 1, in addition, Bennett discloses that the analyzing step comprises analyzing the information describing the bases to derive the first statistical distribution (Section 2, note pages 4-5).

Regarding Claim 37,

Claim 37 is a method claim that is broader than method claim 6 and is rejected for the same reasons.

Regarding Claim 7,

Bennett as modified by Sych discloses the method of claim 1, in addition, Bennett discloses that the establishing step comprises determining a statistical error rate (Section 2, note pages 4-5; and Sections 4-5).

Regarding Claim 38,

Claim 38 is a method claim that is broader than method claim 7 and is rejected for the same reasons.

Regarding Claim 10,

Bennett as modified by Sych discloses the method of claim 1, in addition, Bennett disclose that the subset information transmitting step

comprises transmitting the subset information over a public channel, such as a radio channel (Section 2, note pages 4-5).

Regarding Claim 31,

Claim 31 is a method claim that is broader than method claim 10 and is rejected for the same reasons.

Regarding Claim 11,

Bennett as modified by Sych discloses the method of claim 1, in addition, Bennett discloses that the deriving step comprises transmitting information to the recipient representing the bases for the quantum states not in the subset which make up the first binary string (Section 2, note pages 4-5).

Regarding Claim 41,

Claim 41 is a method claim that is broader than method claim 11 and is rejected for the same reasons.

Regarding Claim 12,

Bennett as modified by Sych discloses the method of claim 1, in addition, Bennett discloses that carrying out the reconciliation step comprises using privacy amplification techniques (Section 2, note pages 8-9).

Regarding Claim 42,

Claim 42 is a method claim that is broader than method claim 12 and is rejected for the same reasons.

Regarding Claim 13,

Bennett as modified by Sych discloses the method of claim 1, in addition, Bennett discloses that the quantum entity is photons and the quantum states are degrees of polarization of the photons (Section 2, note pages 4-5); and Sych discloses that the quantum entity is photons and the quantum states are degrees of polarization of the photons (Pages 4-8, Section III).

Regarding Claim 32,

Claim 32 is a method claim that is broader than method claim 13 and is rejected for the same reasons.

Regarding Claim 43,

Claim 43 is a method claim that is broader than method claim 13 and is rejected for the same reasons.

Regarding Claim 16,

Bennett as modified by Sych discloses the method of claim 1, in addition, Bennett discloses determining the second plurality of bases independently of the first plurality of bases (Section 2, note pages 4-5); and Sych discloses determining the second plurality of bases independently of the first plurality of bases (Pages 4-8, Section III).

Regarding Claim 17,

Bennett as modified by Sych discloses the method of claim 1, in addition, Bennett discloses that the first and second pluralities of bases

are selected randomly (Section 2, note pages 4-5; and Section 3, note page 11); and Sych discloses that the first and second pluralities of bases are selected randomly (Pages 4-8, Section III).

Regarding Claim 18,

Bennett as modified by Sych discloses the method of claim 1, in addition, Bennett discloses the recipient transmitting some information about the bases chosen for measurement and/or the measurement results to the sender (Section 2, note pages 4-5).

Regarding Claim 47,

Claim 47 is a method claim that is broader than method claim 18 and is rejected for the same reasons.

Regarding Claim 19,

Bennett as modified by Sych discloses the method of claim 1, in addition, Bennett discloses that the step of carrying out the reconciliation comprises using several quantum states to generate a single bit of the shared secret at both the sender and recipient (Section 2, note pages 6-9; and Section 5).

Regarding Claim 34,

Claim 34 is a method claim that is broader than method claim 19 and is rejected for the same reasons.

Regarding Claim 48,

Claim 48 is a method claim that is broader than method claim 19 and is rejected for the same reasons.

Regarding Claim 20,

Bennett as modified by Sych discloses the method of claim 1, in addition, Bennett discloses transmitting data regarding the second statistical distribution from the recipient to the sender (Section 2, note pages 4-5).

Regarding Claim 49,

Claim 49 is a method claim that is broader than method claim 20 and is rejected for the same reasons.

Regarding Claim 22,

Bennett as modified by Sych discloses the method of claim 1, in addition, Bennett discloses that each of the plurality of random quantum states defines two-dimensional information describing the condition of the quantum entity (Section 2, note pages 4-5; and Section 3, note page 10).

Regarding Claim 23,

Bennett as modified by Sych discloses the method of claim 1, in addition, Bennett discloses that each of the plurality of random quantum states define n-dimensional information describing the condition of the quantum entity, where n is three or more (Section 2, note pages 4-5; and Section 3, note page 10).

Regarding Claim 24,

Bennett as modified by Sych discloses the method of claim 1, in addition, Bennett discloses that the plurality of random quantum states are arranged geometrically to be uniformly separated within Hilbert space (Section 2, note pages 4-5).

Regarding Claim 33,

Bennett as modified by Sych discloses the method of claim 26, in addition, Bennett discloses that the first plurality of bases is selected randomly (Section 2, note pages 4-5; and Section 3, note page 11); and Sych discloses that the first plurality of bases is selected randomly (Pages 4-8, Section III).

Regarding Claim 46,

Bennett as modified by Sych discloses the method of claim 45, in addition, Bennett discloses that the recipient's plurality of bases is selected randomly (Section 2, note pages 4-5; and Section 3, note page 11); and Sych discloses that the recipient's plurality of bases is selected randomly (Pages 4-8, Section III).

Claims 8, 9, 21, 25, 39, and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bennett in view of Sych, further in view of Black (Black et al., "Quantum Computing and Communication", 2/20.2002, pp. 1-52).

Regarding Claim 8,

Bennett as modified by Sych discloses the method of claim 1, in addition, Bennett discloses that the establishing step comprises determining a degree of difference between the first and second statistical distributions (Section 2, note pages 6-8; and Pages 20-23); but does not explicitly disclose accepting the security of the channel if a degree of correlation between the two distributions is greater than a threshold level.

Black, however, discloses that the establishing step comprises determining the degree of difference between the first and second statistical distributions; and accepting the security of the channel is the degree of correlation between the two distributions is greater than a threshold level (Pages 35-36). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the error checking technique of Black into the QKD system of Bennett as modified by Sych in order to provide the ability to start over with a completely new key in the event that the error rate is too high, which could indicate a possible interception by an eavesdropper.

Regarding Claim 39,

Claim 39 is a method claim that is broader than method claim 8 and is rejected for the same reasons.

Regarding Claim 9,

Bennett as modified by Sych and Black discloses the method of claim 9, in addition, Black discloses selecting the value of the threshold level (Pages 35-36).

Regarding Claim 40,

Claim 40 is a method claim that is broader than method claim 9 and is rejected for the same reasons.

Regarding Claim 21,

Bennett as modified by Sych does not disclose determining the size of the shared secret to be of the same order as the size of a message to be encrypted with the key.

Black, however, discloses determining the size of the secret shared key to be of the same order as the size of a message to be encrypted with the key (Pages 30-31). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the OTP of Black into the QKD system of Bennett in order to obtain complete security in encryption, such that there is no way to determine a match between the encrypted message and the key.

Regarding Claim 25,

Bennett as modified by Sych discloses a secure communications method for conveying a message from a sender to an intended recipient, the method comprising establishing a shared secret random cryptographic key between a sender and a recipient using a quantum communications

channel according to a method as described in claim 1 (see above rejection of claim 1);

But does not disclose using the shared secret key as a one time pad for secure encryption of the elements of the message at the sender; transmitting the encrypted message to the intended recipient using a conventional communications channel; and using the shared secret key as a one time pad for secure decryption of the encrypted elements of the message at the recipient.

Black, however, discloses using the shared secret key as a one time pad for secure encryption of the elements of the message at the sender; transmitting the encrypted message to the intended recipient using a conventional communications channel; and using the shared secret key as a one time pad for secure decryption of the encrypted elements of the message at the recipient (Pages 30-31). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the OTP of Black into the QKD system of Bennett in order to obtain complete security in encryption, such that there is no way to determine a match between the encrypted message and the key.

Claims 14, 15, 44, and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bennett in view of Sych, further in view of Franson (U.S. Patent 6,678,450).

Regarding Claim 14,

Bennett as modified by Sych does not disclose temporarily storing the received quantum states of the quantum entity prior to carrying out the measuring step.

Franson, however, discloses temporarily storing the received quantum states of the quantum entity prior to carrying out the measuring step (Column 29, line 16 to Column 30, line 31; storage of the quantum entity inherently occurs before the measuring of Bennett as modified by Sych). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the quantum entity storage of Franson into the QKD system of Bennett as modified by Sych in order to allow for caching of information, such that the system can store new quantum information while measuring and processing older quantum information, thereby increasing reliability that data will not be lost.

Regarding Claim 44,

Claim 44 is a method claim that is broader than method claim 14 and is rejected for the same reasons.

Regarding Claim 15,

Bennett as modified by Sych and Franson discloses the method of claim 14, in addition, Franson discloses that the measuring step is carried out after the temporary storing step (Column 29, line 16 to Column 30, line 31); and Bennett discloses using the received recipient composition

information to determine some of the bases of the second plurality of bases (Section 2, note pages 4-6).

Regarding Claim 45,

Claim 45 is a method claim that is broader than method claim 15 and is rejected for the same reasons.

(10) Response to Argument

Appellant argues on pages 10-11, regarding claim 1, that Bennett does not disclose that a statistical distribution is derived from composition information describing a subset of transmitted random quantum states or that a second statistical distribution is derived from composition information describing a subset of measured and received random quantum states, that the two sets of statistical distributions are analyzed to verify whether the sets of statistical distributions are sufficiently similar, or that a first binary string is derived from transmitted quantum states not in the earlier subset or that a second binary string is derived from received quantum states not in the earlier subset.

It is first noted that Appellant states on page 10 of the Appeal Brief directly before these arguments, with respect to Bennett, that "Alice and Bob keep only the data from these correctly-measured photons and discard the rest. The remaining cases are then translated into bits (1's and 0's) and thereby become the key." The data created from the correctly measured photons does not directly become the key as Appellant contends, however, there is much processing performed after such base agreement

communication. This additional processing is detailed below in regard to the limitations that Appellant's argues.

The communicating parties, Alice (the sender) and Bob (the receiver) communicate information regarding which measurements were made in the correct bases by Bob, discarding those results that were measured with wrong bases. The parties then compare polarizations of a random subset of the photons to estimate an error rate (level of confidence in the validity of the data) and determine whether the data is sufficiently similar and, therefore, usable. This will determine whether the measurements that Bob made correspond to the data that Alice sent. This step uses the well-known properties of Quantum communication, described in the first full paragraph of Bennett, page 4, in that measuring one property of a quantum entity (e.g. photon) necessarily randomizes the value of other properties of the quantum entity. This means that once the property (e.g. polarization) of a photon is measured (say, by an eavesdropper), it changes properties of the photon such that the intended recipient can no longer be assured of proper polarization, even when using the proper base for measurement. Therefore, if there are no discrepancies found, the communicating parties (Alice and Bob in this scenario) may safely conclude that there are few or no errors in the remaining uncompared data and that little or none of it is known to any eavesdropper (Bennett, bottom of page 5 to top of page 6). This clearly teaches using composition information describing a subset of the quantum states (the bases and/or polarization of the quantum states) and the quantum states that Bob has measured/received to derive statistical distributions, one describing the subset of

transmitted quantum states (from Alice, the sender), and one describing the subset of measured quantum states (from Bob, the receiver). This data is then compared in order to determine whether they are sufficiently similar. If they are sufficiently similar, the protocol progresses. If not, there are too many errors, indicating an eavesdropper's presence and/or noise in the communications channel and/or equipment.

After this stage of Bennett's protocol, the parties begin reconciliation based on error correction of Alice's and Bob's strings of bits (reconciliation begins at the top of page 7). This stage comprises partitioning the data into blocks of equal size at both Alice and Bob, and comparing the block's parity. If the parity matches, the blocks are tentatively accepted as correct, pending additional processing down the line. If the parity does not match, however, the errors are found and corrected. Every time a block is checked for parity, the last bit of the block is discarded. As can be seen, this portion of the protocol clearly teaches deriving correlated binary strings (one at the sender, Alice, and one at the receiver, Bob, the bits being defined on page 5 and dependent upon each photon's polarization), and carrying out reconciliation of the bit strings by use of error correction techniques in order to establish a shared key from the strings.

As discussed above, there is a random subset of data chosen for which Alice and Bob compare the photon polarization in order to estimate an error rate of the data not within this subset. In footnote[3] of page 7, this is further described in that "a small random sample of the bits could be compared initially in order to estimate the error rate, much like the quality control mechanism in the basic quantum key distribution protocol. Of course, these bits would then have to be sacrificed." From here it is quite clear that

the data used in the bit strings to be reconciled includes data that is not included in the subset and compared in this step.

Further disclosure of such limitations may be found within Sych. Page 5 (paragraph immediately following step 3 of the QC-protocol), for example, describes that "When transmission of the message is completed, Alice and Bob disclose part of the measurement results transmitting them over an insecure classical channel in order to determine the mutual probability distribution, which is then used for calculation of an average amount of transmitted information per an elementary step of the QC-protocol. After that, disclosed results are discarded and not used for further generation of a secret key. If the security condition (8) is fulfilled, Alice and Bob decide that the secret key transfer is completed, otherwise the transmitted key is not used." Security condition (8) is a condition ensuring that the amount of information that Bob has received from Alice exceeds the amount of information an eavesdropper received from either Alice or Bob. This portion of Sych clearly teaches analyzing statistical distributions and establishing a level of confidence by verifying that the distributions are sufficiently similar, discarding the data from the subset, and using the data not in the subset in generation of the key.

No additional arguments are made regarding the other claims and rejections, however, a few discrepancies arise. On page 14, for example, Appellant argues with respect to claim 26, that Bennett does not disclose "that a statistical distribution is derived from composition information describing a subset of transmitted random quantum states or that a second statistical distribution is derived from composition information describing a subset of measured and received random quantum entities",

that Bennett also does not describe "that the two sets of statistical distributions are analyzed to verify whether the sets of statistical distributions are sufficiently similar", and that Bennett does not disclose "that a second binary string is derived from received quantum states not in the earlier subset." None of these limitations are within claim 26 and it is not understood why they are discussed here. Appellant then concludes "For at least these reasons, *Bennett* fails to teach or suggest "transmitting to the recipient composition information describing a subset of the plurality of random quantum states [and] deriving a first binary string from the transmitted plurality of quantum states not in the subset". From the above discussion of claim 1, it is clear that both Bennett and Sych teach such limitations.

As with claim 26, Appellant argues limitations regarding claim 35 that are not claimed. On page 18, for example, Appellant argues that Bennett does not disclose "that a first binary string is derived from transmitted quantum states not in the earlier subset or that a second binary string is derived from received quantum states not in the earlier subset." Claim 35 does contain the limitation of "deriving a recipient binary string from the received plurality of quantum states not in the subset", however, there is only this one string in claim 35, not first and second binary strings as Appellant argues. From the above discussion of claim 1, it is clear that the combination of Bennett in view of Sych teaches all limitations of claim 26.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Jeffrey D Popham/
Examiner, Art Unit 2137

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132

Conferees:

/G. B./
Supervisory Patent Examiner, Art Unit 2132

/Benjamin E Lanier/
Primary Examiner, Art Unit 2132